General Data Protection Regulation: Take Home Points for FGB Researchers

- Regulates processing of personal data from natural persons
    - Data processing means ALL data-related activities
        - Collecting
        - Adapting
        - Storing
        - Analysing
        - Destroying
    - Personal data is more than just name and contact information. It is any information that can be linked back to a unique individual
- Does not apply to deceased individuals or legal persons (e.g. Corporations)
- Does not apply to anonymous data
    - NOTE: completely anonymous data is very difficult to achieve; information about a person other than name and contact information can still allow for re-identification
- Applies to all personal data processed by researchers of the VU, regardless of whether the processing takes place in the EU or not.
    - NOTE: Countries outside of the EEA (EU + Iceland, Norway and Liechtenstein) may have their own privacy laws which compliment or supersede the GDPR
- The Stichting VU is, in most cases, defined as the data controller; the controller decides the purpose and aims of the processing
    - All activities that carried out within the VU must meet the legal obligations of a controller
    - When working with other institutions that have their own purposes and aims, a joint controller agreement must be established
- Data processing must be lawful. Lawful grounds appropriate to research are:
    - Informed, freely given consent from participants prior to starting research is still the most appropriate ground for data processing, however requirements for consent are now stricter:
        - Refusal of consent without consequence and revoking of consent at any time without consequence still apply and must be mentioned at the time of consent.
        - Consent must not be passive, i.e. it should not be based on an "opt-out" scheme, where an individual is registered as having given consent until they actively revoke that consent.
        - Specific information must be mentioned at the time of consent. New templates are being developed by the faculty to meet these requirements. The required information is found in article 13 of the GDPR.
        - Consent must be broken down by purpose. Participants must have the option to consent to separate parts of research, but this must be balanced against the aims of the research. If it is necessary to have all participants give a blood sample AND complete a questionnaire to achieve the research aims, simply request consent to both data collections in one question, while ensuring that participants understand that they are consenting to both data collections. If the aims can be achieved even if participants only provide blood OR questionnaire responses, then consent to these two purposes must be requested separately.

OR

    - Demonstrate a legitimate interest for processing data that outweighs the rights of the data subject (the person from whom the data are obtained). For more information and advice on this topic, contact the research data officer for FGB.
- Data that are publicly available (e.g. on Facebook) are not free to use. There must still be lawful reasons to use such data. For more information and advice on this topic, contact the research data officer for FGB.
- If processing special data for research (namely ethnicity, sexuality, health data, genetics, biometrics, religion, political opinions, and trade union memberships), at least one of the following must apply:
    - Explicit, freely given and prior informed consent is obtained from participants

OR

    - (*Only in the Netherlands*) Data are being processed exclusively for scientific purposes AND:
        1. the scientific research is conducted in the public interest;
        2. the processing of the personal data is necessary for the research;
        3. asking for explicit consent has proven to be impossible or would involve disproportionate

effort; **and**

4. the processing is conducted with appropriate safeguards that ensure that privacy of the participant(s) will not be affected disproportionately

- In the Netherlands, research is exempt from most of the data subject rights described in the GDPR. Those which do apply to research are:
  - Subjects must be made aware of any data processing activities. See RDM Policy for FGB Annex 1 for specifics. Templates for creating forms with the required information are being developed. The required information is found in article 13 and 14 of the GDPR.
  - Right to erasure of data: see RDM Policy for FGB Annex 1 for specifics
  - Right to data portability: see RDM Policy for FGB Annex 1 for specifics
  - Right to object to processing: if legitimate interests rather than consent serve as the legal ground for research, participants have the right to object. For more information and advice on this topic, contact the research data officer for FGB.
  - Research is exempt from the right of access (article 15), the right to rectification (article 16) and the right to restriction (article 18) as long as data are being used for solely for scientific research purposes and are appropriately safeguarded, and as long as researchers remain transparent about the use of the data
  - Should an individual ever wish to exercise any one of his or her rights, **including** the rights for which research is exempt, the individual must be referred to the Data Protection Officer for the VU
- Researchers must process only the data that are needed to achieve your research aims; do not collect data just for the sake of it
- Ensure data are accurate: using a research data management plan to organize your data processing and storage mechanisms will help in the achievement of this requirement
- Pseudonymize research data as soon as possible. This means removing all directly identifying information (e.g. names, contact information) from research data.
  - Note that sometimes directly identifying data must be maintained for the duration of the study; if this is the case it should be stored separately from the research data. See RDM Policy for FGB Annex 1 for specifics
- Establish appropriate technical and organizational measures that protect data and prevent unauthorized access:
  - Determine who has access to which data and keep this information up-to-date
  - Process data in secure locations
  - Ensure that third party processers have signed data processing agreements.
    - If a new agreement is necessary, use the VU model agreement and start the process early. The Faculty Director is the only FGB staff member allowed to sign this document.
  - If sharing data with non-EU countries, ensure that they have met the adequacy standards of the EU commission or sign a standard contractual clause for data transfers
    - Data transfers include storage of data on servers outside of the EEA as well as sending data to parties outside of the EEA
  - If a possible data breach occurs, inform the IT Service Desk immediately (servicedesk.it@vu.nl or +31 20 59 8000)
    - Data breach examples include: a lost USB stick, a hacked VU account, e-mailing sensitive information to the wrong e-mail address, a stolen laptop etc.
- Maintain a register of your data processing activities
  - Within the VU, this will be performed using PrivacyPerfect (https://vu.privacyperfect.com)
- Assess the need for a data protection impact assessment before starting processing
  - PrivacyPerfect will assist researchers in this assessment and in the completion of DPIAs.
- Additional information:
  - There are many specific details and exemptions not listed here
    - Additional information provided by the Data Protection Officer for the VU can be found here
  - The GDPR text can be reviewed here
  - The UAVG, the local implementation legislation, can be reviewed here
  - Additional information from the local Data Protection Authority is available here